REMARKS

These remarks are made responsive to the non-final office action mailed July 13, 2007. Claims 1-25 are pending.

35 U.S.C. § 102(e)

Claims 1 and 3-9 were rejected under 35 U.S.C. 102(e) as being anticipated by Mackay et al. (US 7,107,448) hereafter "Mackay." Applicant respectfully asserts that claims 1 and 3-9 are patentable over Mackay.

Mackay is concerned with enabling content owners to supervise access to electronic content. "If it determined that the second application is not adequately enforcing the rules, the supervisory management system can revoke the second application's ability to access the content and/or the second application's ability to grant access to the content." (Col. 2, lines 31-35). The invention of claim 1 is directed to a method for safely executing downloaded code on a computer system. The method of claim 1 "validat[es] said requesting thread at said local security filter and return[s] a digital signature that uniquely identifies said requesting thread to said application process." The kernel of the computer system in claim 1 uses "said digital signature from said security filter to validate *said requesting thread* [emphasis added]."

Mackay is not validating threads, but the rights of applications to access rights managed content. (See col. 9, lines 8-12) "The mediator/shim 354 of the conformance library 351 may incorporate additional logic which, e.g. (a) allows it to verify or validate that a legitimate authorization certificate/ conformance certificate has been given by the content owner ..." An implementation example for the Governance engine of Mackay is "InterTrust's InterRights Point software or Rights/System software." Mackay is concerned with making sure an improperly modified application does not have rights to contents for digital rights management purposes, and not for confining threads for safely execution of downloaded code on a computer system.

Applicants respectfully assert that Mackay does not anticipate claims 1 and 3-9, and request that the rejection be withdrawn.

35 U.S.C. § 102(e)

Claims 10-14 and 17-19 were rejected under 35 U.S.C. 102(e) as being anticipated by Charbonneau (US 2003/0074567) hereafter "Charbonneau." Applicant respectfully asserts that claims 10-14 and 17-19 are patentable over Charbonneau. Charbonneau's paragraph [0035] fails to disclose the "method for determining the source of a resource request" as recited in independent claim 10. In its paragraph [0035] Charbonneau discloses that a password for a user is verified. "In use, a user of system 11 initiates an action requiring a password, such as for instance attempting to access a user data file 2 associated with the untrusted application 1." The system in Charbonneau does not generate "a first check value associated with said resource request." Instead, it compares the current state of the applications running within the computer system as represented by a hash value to a trusted hash value retrieved when the system was in a verified secure state. These hash values are not associated with the resource request itself as are the first and second check values of claim 10.

Furthermore, Figure 2 of Charbonneau only indicates "a trusted group of applications" 4. Assuming arguendo that the trusted hash value is considered a "validation secret", Charbonneau fails to illustrate "a security filter comprising a validation secret" and "said system kernel comprising said validation secret." There is no indication these applications are in the kernel space, and likely may be in the application space. Furthermore, the trusted hash value does not appear to be comprised within a security filter or a system kernel.

Applicants respectfully assert that Charbonneau fails to anticipate independent claim 10, and hence its dependent claims 11-19.

35 U.S.C. § 103(a)

Claims 2, 10, 15-16 and 20-25 were rejected under 35 U.S.C. 103(a) as being unpatentable over Mackay and further in view of Charbonneau. Applicant respectfully asserts that claims 2, 10, 15-16 and 20-25 are patentable over Mackay in view of Charbonneau.

The arguments presented above for independent claims 1 and 10 are applicable for illustrating why claim 2 which depends from claim 1 and claim 10 and its dependents 15-16 are patentable over the combination of Mackay in view of Charbonneau.

Furthermore, the combination of Mackay in view of Charbonneau fails to render unpatentable claims 20-25. Neither of these references teaches "a security filter [which] comprises a secret for generating a first digital signature" as well as a "system kernel comprising said secret for generating a second digital signature associated with said resource request."

It is respectfully requested that rejection of claims 2, 10, 15-16 and 20-25 be withdrawn.

Conclusion

In light of the arguments and amendments presented above, the pending claims as amended are in condition for allowance, and applicants respectfully request a prompt notice of allowance.

Date: 01/14/08

Respectfully Submitted on Behalf of Applicants
Alan Karp et al.

Eileen Lehmann

Eileen Lehmann
Registration No. 39,272
Hewlett-Packard Company
Mail Stop 1197
1501 Page Mill Road
Palo Alto, CA 94304
650-857-7940 (telephone)
650-852-8063 (fax)